UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

# REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

**1a. REPORT SECURITY CLASSIFICATION:** Unclassified

**1b. RESTRICTIVE MARKINGS:**

**2a. SECURITY CLASSIFICATION AUTHORITY:**

AD-A207 888

**3. DISTRIBUTION/AVAILABILITY OF REPORT:** Approved for public release; distribution unlimited.

**5. MONITORING ORGANIZATION REPORT NUMBER(S):** AFOSR-TR- 89-0624

**6a. NAME OF PERFORMING ORGANIZATION:** Columbia University

**6b. OFFICE SYMBOL (If applicable):**

**7a. NAME OF MONITORING ORGANIZATION:** AFOSR

**6c. ADDRESS (City, State, and ZIP Code):** Department of Mathematics, Box 20, Low Memorial Lib., New York NY 10027

**7b. ADDRESS (City, State, and ZIP Code):** Building 410, Bolling, AFB DC 20332-6448

**8a. NAME OF FUNDING/SPONSORING ORGANIZATION:** AFOSR

**8b. OFFICE SYMBOL (If applicable):** NM

**9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER:** AFOSR-87-0117

**8c. ADDRESS (City, State, and ZIP Code):** Building 410, Bolling, AFB DC 20332-6448

**10. SOURCE OF FUNDING NUMBERS**

| PROGRAM ELEMENT NO. | PROJECT NO. | TASK NO. | WORK UNIT ACCESSION NO. |
|---|---|---|---|
| 61102F | 2304 | A4 | |

**11. TITLE (Include Security Classification):** Differential Equations, Related Problems of Pade Approximations and Computer Applications

**12. PERSONAL AUTHOR(S):** D. V. Chudnovsky and G. V. Chudnovsky

**13a. TYPE OF REPORT:** Final

**13b. TIME COVERED:** FROM 1 Jan 87 TO 31 Dec 88

**14. DATE OF REPORT (Year, Month, Day):**

**15. PAGE COUNT:** 5

**16. SUPPLEMENTARY NOTATION:**

**17. COSATI CODES**

| FIELD | GROUP | SUB-GROUP |
|---|---|---|
| | | |
| | | |

**18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number):**

**19. ABSTRACT (Continue on reverse if necessary and identify by block number)**


During the past period of the Grant, our work focused on the study of analytic, arithmetic and algorithmic properties of differential equations applied to solutions of problems in theoretical mathematics, mathematical and theoretical physics, numerical methods and computer science.




**20. DISTRIBUTION/AVAILABILITY OF ABSTRACT:** ☐ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

**21. ABSTRACT SECURITY CLASSIFICATION:** Unclassified

**22a. NAME OF RESPONSIBLE INDIVIDUAL:** Dr. Arje Nachman

**22b. TELEPHONE (Include Area Code):** (202) 767-4939

**22c. OFFICE SYMBOL:**

DD Form 1473, JUN 86 — Previous editions are obsolete.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

89 5 15 225

Grant No.
AFOSR-87-0117

AFOSR-TR- 89-0624

# Differential Equations,

# Related Problems of Padé Approximations

# and Computer Applications

~~Final~~ Technical Report

by D.V. Chudnovsky and G.V. Chudnovsky

Department of Mathematics
Columbia University



During the past period of the Grant, our work focused on the study of analytic, arithmetic and algorithmic properties of differential equations applied to solutions of problems in theoretical mathematics, mathematical and theoretical physics, numerical methods and computer science.

The work of the investigators in the area of effective approximation methods in diophantine geometry, differential equations and computer realizations have progressed in several directions. ~~In diophantine~~ approximations we continued to study the relationship is studied between complex-analytic and arithmetic (p-adic) properties of linear differential equations using Padé approximations methods. One of the crucial problems here is the transcendence of the elements of the monodromy matrices of linear differential equations defined over $\mathbf{Q}(x)$ and for linear differential equations over C(x) uniformizing algebraic curves of genus $g \geq 1$ defined over $\mathbf{Q}$. These problems are important to complete our solution of the last remaining cases of the Grothendieck conjecture, and for the determination of the arithmetic nature of accessory parametres and natural parameters

next page

of Teichmuller spaces. In this direction we proved the transcendence of elements of the monodromy matrices of linear differential equtions over $\mathbf{Q}(x)$ in many important cases, see [1]. We have developed and implemented entirely new low complexity algorithms of computations of solutions of (linear) differential equations with arbitrary precision [3-4], [9-10], and new efficient numerical methods of solutions and direct monodromy (Riemann) problem. In the uniformization problem, we conducted extensive analytic analysis and run multiple precision (in thousands of leading digits of floating point) computations with our new algorithms for: a) punctured tori case; b) hyperelliptic cureves of genus g, $2 \leq g \leq 6$; [4], [9]. Our computations showed that in most cases, the curves defined over $\mathbf{Q}$ do not have algebraic accessory parameters and do not have monodromy group represented by matrices from $GL_{2}(\mathbf{Q})$. In particular, the long-standing Whittaker conjecture (1929) on explicit algebraic form of accessory parameters in the hyperelliptic case is wrong for a generic curve. Results of complex-analytic and arithmetic computations clearly indicate [9-10] that accessory parameters are algebraic only in cases when the corresponding Fuchsian group is an arithmetic one, or belongs to a special class of triangle subgroups (like in all the previously known cases when Whittaker conjecture was proved). We are continuing our numerical and analytic work aimed at the development of correct conjectural description of (Teichmuller) parameters.

Another part of our work is aimed at complete determination of all (linear) differential equations having arithmetic sense. In many cases we have been able to show that all these equations "arise from Geometry" (are variations of period structures of algebraic manifolds), [11]. This work of ours is closely connected with the study of the arithmetic properties of classical constants of analysis (such as $\pi$, $\zeta(3)$, $\ln 2$, $\Gamma(1/3)$). The common analytic method in all these studies is the method of Pade approximations to solutions to special linear differential eqautions, see [4], [9], [10], [11]. New identities for classical constants significantly improving on known ones (Ramanujan, etc [10]) have been constructed by us now from modular function. These identities have applications to diophantine approximations and to numerical methods as well, [10].

We continue to develop methods of formal groups arising from Abelian varieties (elliptic curves) defined over Z, $Z_p$, $F_p$ used by us for the study of Tate conjecture, factorization and primality testing [2], and in description of characteristic classes of Spin-manifolds and their applications in superstrings [5], [8]. Our formulas for characteristic classes exressed in terms of modular forms of level 2 were used by Witten and others (cf. [8]) in field theory models. They also reveals new interesting congruences necessary for the construction of conjectured extraordinary K-theories, see [8].

Our methods of multi-point approximations and interpolation led to new very efficient low complexity methods of computations over $\mathbb{Z}$ and over finite fields of large classes of problems expressed in terms of bilinear form. Among the problems were our new algorithms are applied are: fast computations of polynomial multiplications, convolutions, and various finite Fourier transforms, binum operations and other operations in computer algebra. Our methods, [6 - 8], are based on interpolation over algebraic curves and manifolds which we developed, and are connected with algebraic coding theory [6]. In particular, we show that the (multiplicative) complexity of multiplication in the extension K of k of degree n is of the order (2 + o(1)) * n for a finite field k. We are further developing these methods, and applying them to fast solution of partial differential eqautions, fast integral transforms, and to fast bignum computations.

New efficient serial and parallel algorithms were proposed by us for power series computation, continued fraction expansions and the numerical evaluation of solutions of linear differential equations, [3], [4], [9], [10]. Among our results is O(log N) upper bound for the complexity of evaluation of N-th partial fraction in the continued fraction expansion for the large class of algebaric functions [4]. Of practical importance are new $O(N \log^2 N) - O(N \ln^3 N)$ algorithms for evaluation with the precision N of a solution of a linear differential equation at an N-digit floating number. Some of these methods were already used by us in monodromy group comutations (see above). Efficient hardware realization of these methods for special functions computations looks very promising, and are under development by us.

Investigators were among organizers (D.V. was a co-chairmen

and G.V. was a member of the Organizing Committee) of an International Conference "Computers and Mathematics" held at Stanford University in July - August 1986. The investigators were members of the Oragnizing Committee of the 1987 AMS Summer School on Theta-Functions (Bowdoin College, Maine, July-August 1987). The investigators were among organizers and speakers of a symposium "Computer Algebraic Integration and Solution of Differential Equations" (I.B.M. Research, Yorktown Heights, November 1987). The investigators co-chair with H. Cohn and M. Nathanson the New York Number Theory Seminar, which has recently published a new volume of its Proceedings: Lecture Notes in Math., v. 1240, Springer, 1987.

## LIST OF PUBLICATIONS OF D.V. CHUDNOVSKY AND G.V. CHUDNOVSKY FOR 1986 - 1987 SUPPORTED BY THE AIR FORCE


1. A random walk in higher arithmetic.
   Advances in Applied Mathematics, v. 7 (1986), 101-122.

2. Sequences of numbers generated by addition in formal groups and new primality and factorization tests.
   Advances in Applied Mathematics, v. 7 (1986), 187-237.

3. On expansion of algebraic functions in power and Puiseux series, Parts I and II.
   J. of Complexities v. 2 (1986), 271-294, and v. 3 (1987), 1-25.

4. Computer assisted number theory.
   I.B.M. Research Report, RC 12030, 7/23/86, 67pp. Lecture Notes in Mathematics, Springer, N.Y., v. 1240, 1987, 1-68.

5. Elliptic modular functions and elliptic genera.
   Topology, 1987.

6. Algebraic complexities and algebraic curves over finite fields.
   Proc. Natl. Acad. Sci. U.S.A., v. 84 (1987), 1739-1743.

7. Algebraic complexities and algebraic curves over finite fields.
   I.B.M. Research Report, RC 12605, 3/24/87, 50pp. J. of Complexities (to appear).

8. Elliptic Formal Groups over $\mathbf{Z}$ and $\mathbf{F}_p$ in Applications to Number Theory, Computer Science and Topolgy.
   I.B.M. Research Report, RC 13318, 8/28/87, 44 pp. Lecture Notes in Mathematics, Springer, 1987.

9. Computer Algebra in the Service of Mathematical Physics and Number Theory.
   Proceedings of 1986 Stanford Conference "Computers and Mathematics", 105 pp. (to appear).

10. Approximations and complex multiplication according to Ramanujan.
    Proceedings of the Ramanujan Centenary Conference, 97 pp., Academic Press, 1987.

11. Transcendental Methods and Theta-Functions.
    Proceedings of the A.M.S. 1987 Summer School on Theat-Functions, Proc. Symp. Pure Math., A.M.S., Providence (to appear).